IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
CHARLOTTESVILLE DIVISION

IN THE MATTER OF THE SEARCH OF
1321 VILLA WAY, UNIT F,
CHARLOTTESVILLE, VIRGINIA 22903

Case No. 3:25-mj-12

Filed Under Seal

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jade S. Laughlin, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since March 2015. I am currently assigned to the FBI Richmond Field Office, Charlottesville Resident Agency. As part of my duties as an FBI SA, I have investigated criminal violations relating to international organized crime, homicides on federal lands, drug trafficking organizations, crimes against children, and other various criminal matters. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence identification, child pornography identification, computer evidence seizure and processing, and various other criminal laws and procedures.

2. This affidavit is submitted in support of an application for a search warrant pursuant to Rule 41 of the Rules of Criminal Procedure for the premises located at **1321 Villa Way, Unit**

F, Charlottesville, VA 22903 (the "SUBJECT PREMISES"), for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B), which items are more specifically described in Attachment B of this affidavit.

3. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent with the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections § 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

b. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "**Illicit sexual conduct**" means, in relevant part, a sexual act (as defined in section 2246), with a person under 18 years of age that would be in violation of chapter 109A if the sexual act occurred in the special maritime and territorial jurisdiction (SMTJ) of the United States. Under 18 U.S.C. § 2243, an offense under Chapter 109A, it is a crime for a person to knowingly engage, or attempt to engage, in a sexual act, as defined in 18 U.S.C. § 2246(2) with someone who has attained the age of 12 but not 16, when the minor is at least four years younger than the offender (in the SMTJ). Under 18 U.S.C. § 2244(a)(3), another Chapter 109A offense, it is a crime to engage in "sexual contact," as defined in 18 U.S.C. 2246(3), with a minor, at least four years younger who is between 12 and 15 years of age in the SMTJ.

b. "**Child Pornography**" includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

c. "**Visual depictions**" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

d. "**Minor**" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

e. "**Sexually explicit conduct**" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

f. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical,

electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, VHS tapes, mini-cassette tapes, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

6. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "Collectors").

7. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

8. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

9. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

10. Collectors may possess and maintain their "hard copies" of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the Collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the legal and social danger associated with acquiring them. As a result, it is not uncommon for Collectors to hoard and retain child pornography for long periods of time, even for years.

11. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

12. Producers of child pornography are even more likely to keep images or videos that they have created. This is because while pornographic images of anonymous images could possibly be replaced with images of other anonymous children, such as when "culling" a collection to improve the overall quality, images and videos of sexual acts depicting both the individual and known children are irreplaceable. Based upon my knowledge, training, and experience, producers of child pornography rarely, if ever, delete child pornography from a private collection.

BACKGROUND AND USE OF THE "KIK MESSENGER"

13. Kik Messenger, also known as "Kik," is a popular free instant messenger

application (app) for mobile devices (i.e. smart cell phones, tablets, iPods, etc.) which was previously owned by the Canadian company, Kik Interactive, which was founded in 2009. Kik was acquired by Media Lab, a Los Angeles based company in 2019. Kik is available on several mobile device platforms including, iOS, Android, and Windows Phone operating systems. The Kik application can be located through Google's "Play Store," and Apples "App Store." The Kik application utilizes the internet connection through the mobile devices' data plan or through Wi-Fi, to transmit and receive messages, photos, videos, sketches, mobile webpages, and other content transmitted by through the Kik application. Kik allows its users to register an user account without providing a telephone number, and prevents users from being located on the service through any information other than their chosen unique Kik username.

14. After locating the Kik application and downloading the application to the mobile device, the application requests permission to access the following data on the mobile device during the installation process: in-app purchases, identity, contacts, location, photos/media/files, camera, microphone, device ID & call information. Once given permission by the user, the Kik application installs itself on the mobile device. After installing the Kik app on the mobile device and initializing the Kik application for the first time, the potential user is required to establish a Kik account and is prompted to select the "SIGN UP" option. While establishing a Kik account, the potential user is prompted to provide information, including the user's "First Name," "Last Name," and "Birthday." The potential user is prompted to create a "Kik Username," (which is the only information that is required to be unique,) and is prompted to provide an "Email address." The information provided by the potential user is used to establish a Kik account; however, this user information is not verified and the information can be completely fictitious (except for the uniqueness of the Kik username). A "verification email" is sent by Kik to the user's provided

email address and the user is prompted to verify the email address. Verification of the user's email address is not required and does not prevent the user from utilizing the application if not verified. The potential Kik user is prompted to provide a user profile picture, which can either be taken using the mobile device's camera feature or uploaded from the device photo gallery. However, the lack of a profile picture does not prevent the user from utilizing the application. The Kik username is created by the user and is the only information that is required to be unique.

15. At the completion of the account registration, the user is allowed to start communicating with other Kik users. Searching for specific Kik users can only be performed using the Kik user's registered "username;" searches by phone number or email address cannot be performed. Entering the unique Kik username through the application's search field yields potential matches in which the user simply selects the Kik user to start communicating with that specific user.

16. In today's world where mobile phones are the technology of choice for millions of people to communicate, chat applications like Kik Messenger are often used to communicate with others, and on occasions are used during the commission of crimes, like the online harassment and bullying of juveniles, and the sexual exploitation of minors. Mobile devices which utilize social media and communication applications, store, or "cache," certain data from the social media or communication applications directly on the mobile device and this data can be recovered by a forensic expert. The Kik Messenger application is no different.

17. For both iOS and Android devices, most Kik artifacts relevant to criminal investigations are stored within specific databases located in specific locations on the mobile devices. These databases store details concerning the Kik users' contacts, messages, and attachments sent and received through the Kik Messenger application. These databases contain

such data as the usernames and display names for each contact, but are not limited to this type of information. The Kik username is a unique identifier for each and every Kik user and this type of data is valuable in criminal investigations. The Kik contact database can also contain profile picture links and timestamps, as well as group and block lists. This data can be recovered from the mobile device by trained computer experts.

18. Messages, including any attached image files, are stored within a specific location on the mobile device, depending on the device used. As Kik stores all of its data in this specific location within the mobile device, in an unencrypted format, there is a good chance that the entire messaging history, if not a partial message history, can be recovered by trained computer experts and used during investigations.

19. Users sometimes delete their conversation histories by clearing the Kik Messenger logs. However, since the Kik messaging databases are not wiped or erased immediately (depending on the operating system of the mobile device), these deleted records end up being stored in a specific location in a specific format on the mobile device. These deleted records may be kept for a period of time until the database reclaims the space to store new records. A forensic expert has the ability to recover such records which could prove useful in various investigations.

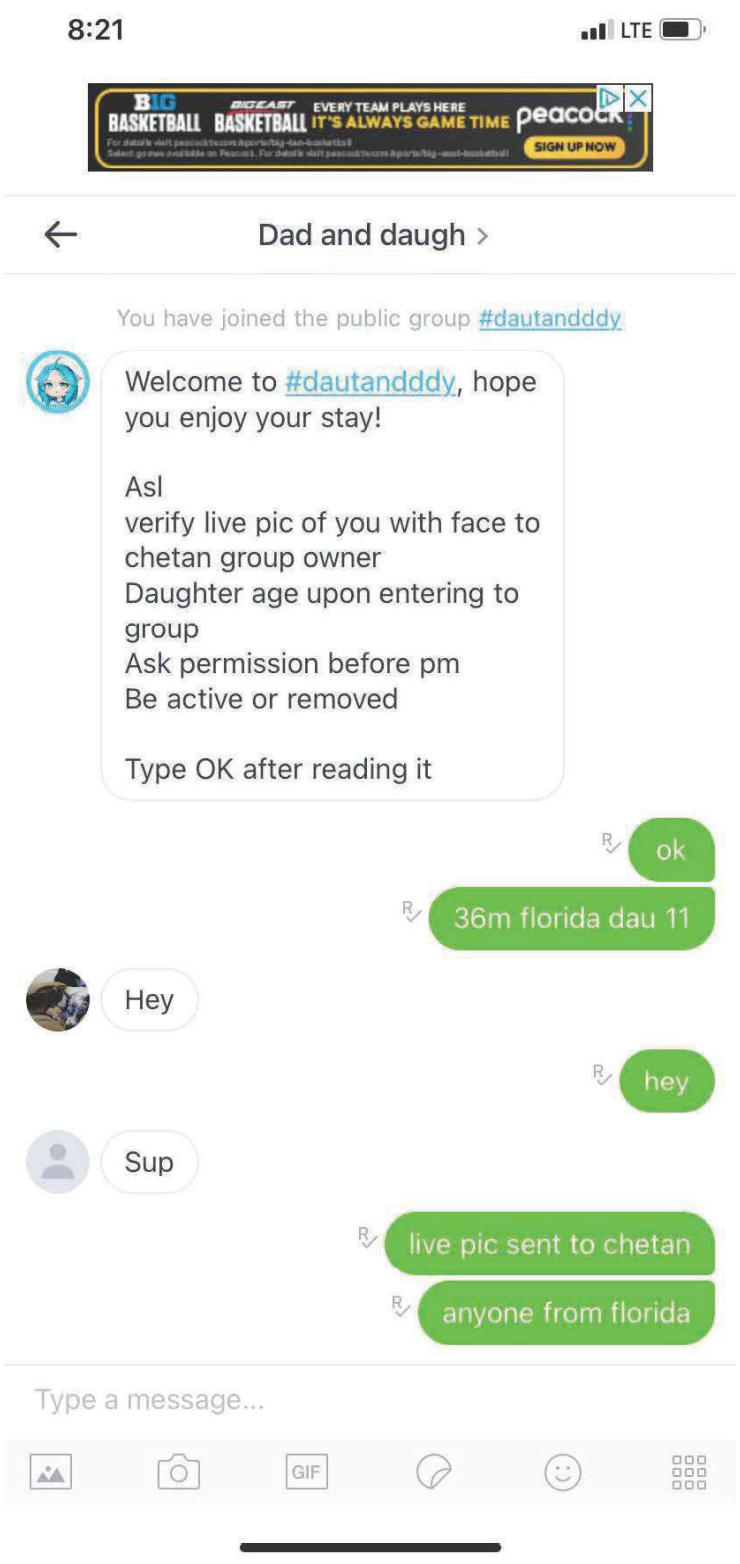
20. Sometimes, a user will attempt to destroy evidence by deleting the database file completely. While there is nothing that can be done to recover this information form an iOS device (the operating system does not allow for the recovery of anything that has been deleted), carving Android and chip-off dumps may return an amazingly high amount of deleted evidence.

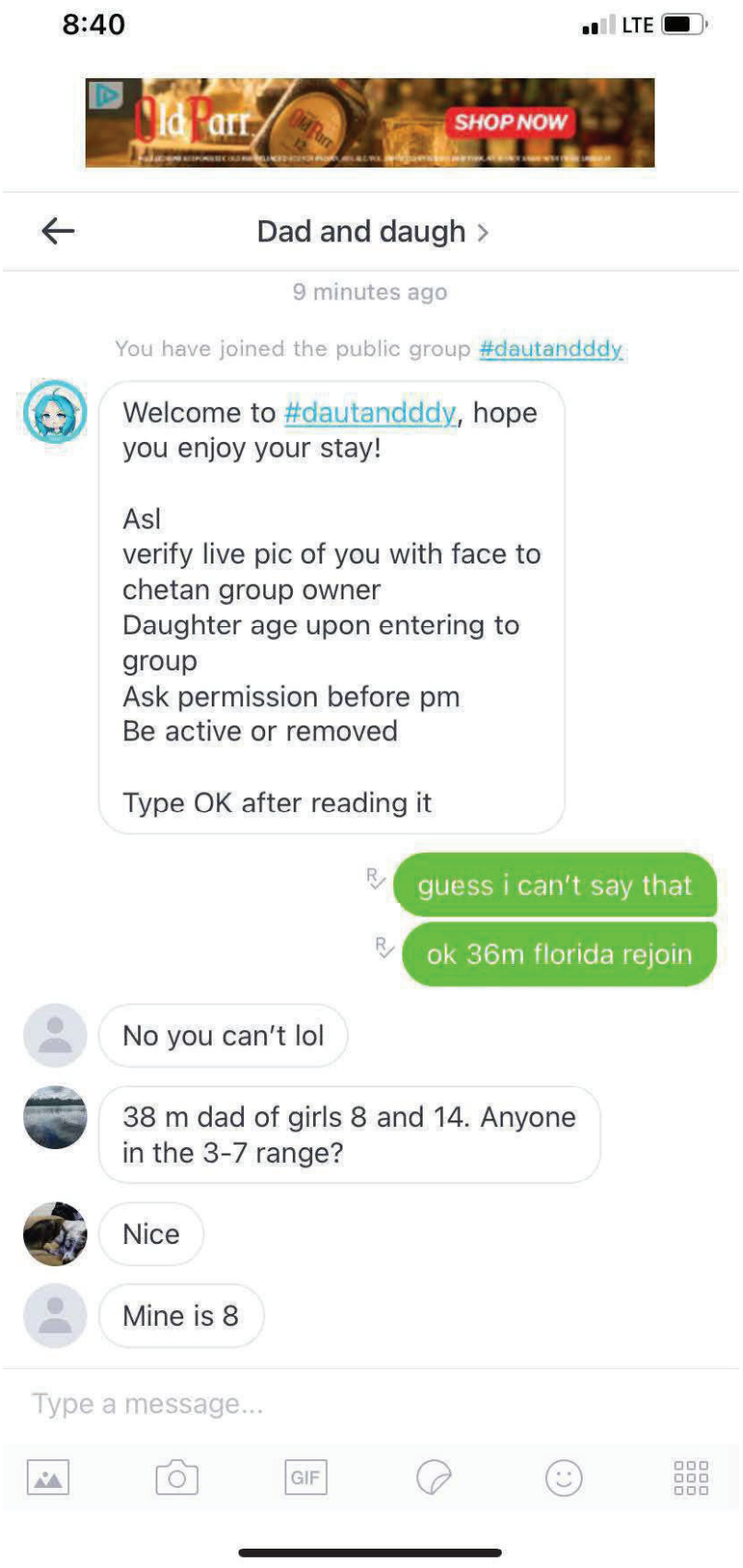
PROBABLE CAUSE

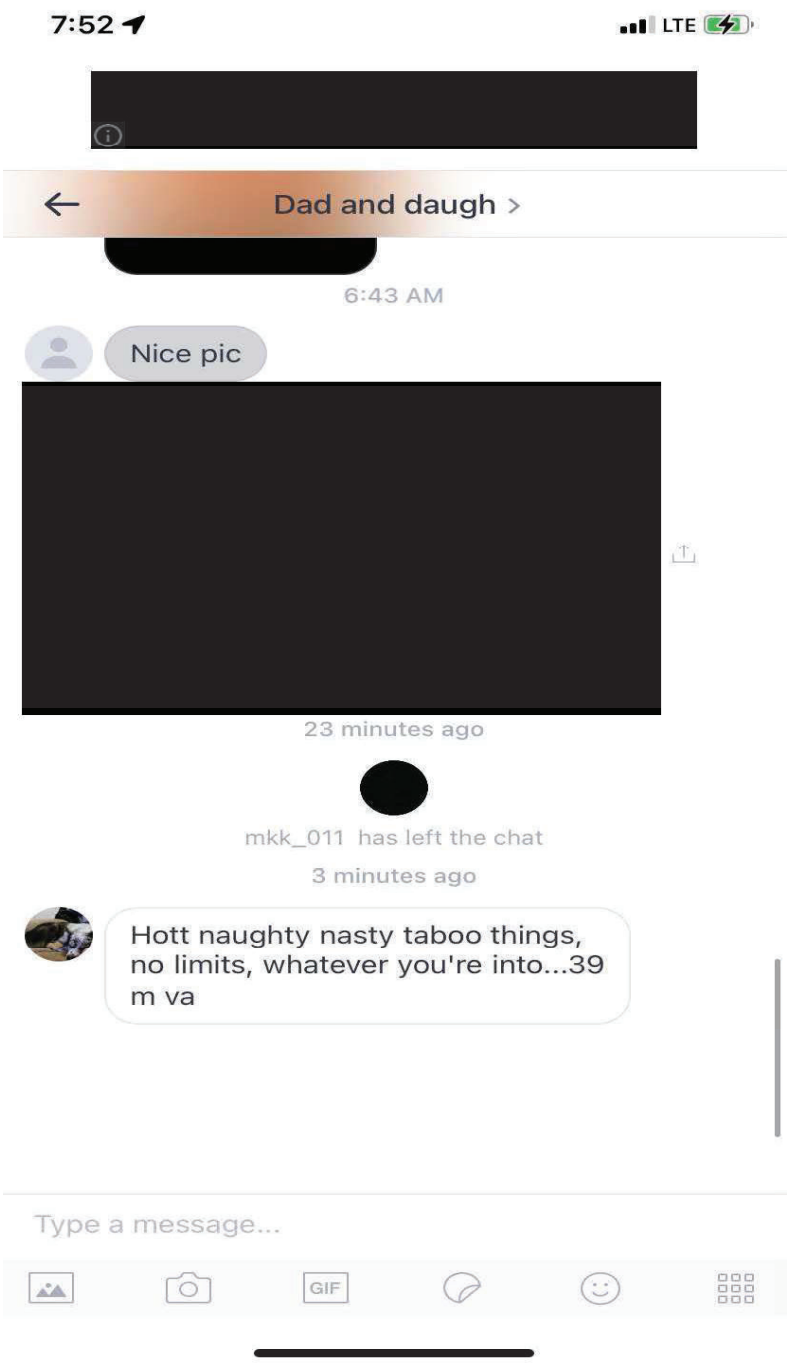
21. During a FBI undercover operation from December 3, 2024 through December 5, 2024, a user utilizing Kik account “27mav” exchanged messages with a FBI Online Covert

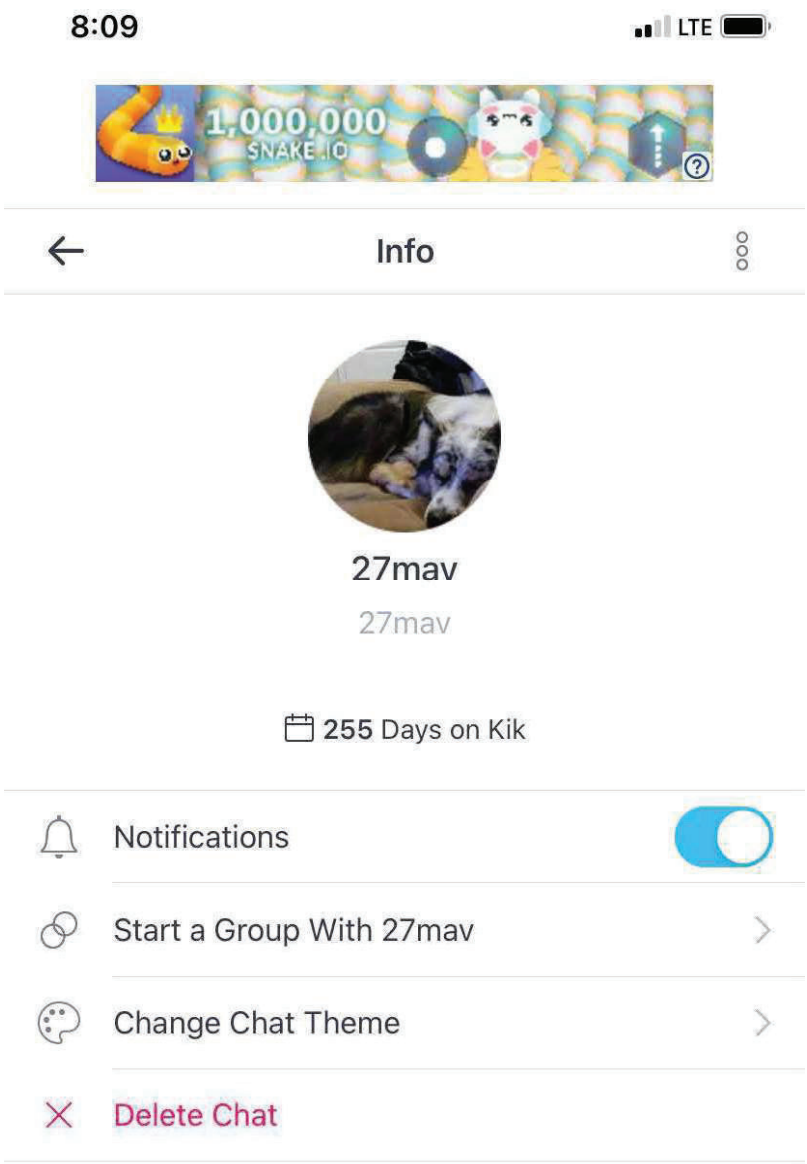
Employee (OCE). The user of 27mav had the following conversation (pasted below) via Kik with the FBI OCE within a "Dad and daugh" public chat group identified by the hashtag #dautandddy. Based on my training and experience, this chat group and others are focused on fathers who have a daughter, often referred to as "daug". Based on my training and experience, individuals in these groups have a sexual interest for minors. The individuals often share Child Sexual Abuse Material (CSAM) in photographic and/or video form of their purported daughter(s). Many individuals in these type forums will trade photographs and/or videos. Individuals may ask to "share daug" as indicator. For example, one may share an explicit photograph of his daughter and in kind expect the other individual to share an explicit photograph of his daughter.

22. During the conversation pasted below, "27mav" stated that he resides in Charlottesville, Virginia. The FBI OCE's comments are shown below in green. "27mav"'s comments are shown below, in white, with the profile photograph of an Australian breed dog. Other users commenting in the group chat are shown with different profile photographs or a gray male symbol. Photographs that have black boxes and markings have been redacted. The chat is pasted below:


8:21
LTE
BIG BASKETBALL
BIGEAST BASKETBALL
EVERY TEAM PLAYS HERE
IT'S ALWAYS GAME TIME
peacock
SIGN UP NOW
Dad and daugh
You have joined the public group #dautandddy
Welcome to #dautandddy, hope you enjoy your stay!
Asl
verify live pic of you with face to chetan group owner
Daughter age upon entering to group
Ask permission before pm
Be active or removed
Type OK after reading it
ok
36m florida dau 11
Hey
hey
Sup
live pic sent to chetan
anyone from florida
Type a message...
GIF


8:40
LTE
Old Parr
SHOP NOW
Dad and daugh
9 minutes ago
You have joined the public group #dautandddy
Welcome to #dautandddy, hope you enjoy your stay!
Asl
verify live pic of you with face to chetan group owner
Daughter age upon entering to group
Ask permission before pm
Be active or removed
Type OK after reading it
guess i can't say that
ok 36m florida rejoin
No you can't lol
38 m dad of girls 8 and 14. Anyone in the 3-7 range?
Nice
Mine is 8
Type a message...
GIF


7:52
LTE
Dad and daugh >
6:43 AM
Nice pic
23 minutes ago
mkk_011 has left the chat
3 minutes ago
Hott naughty nasty taboo things, no limits, whatever you're into...39 m va
Type a message...
GIF


8:09
LTE
1,000,000
SNAKE.IO
Info
27mav
27mav
255 Days on Kik
Notifications
Start a Group With 27mav
Change Chat Theme
Delete Chat

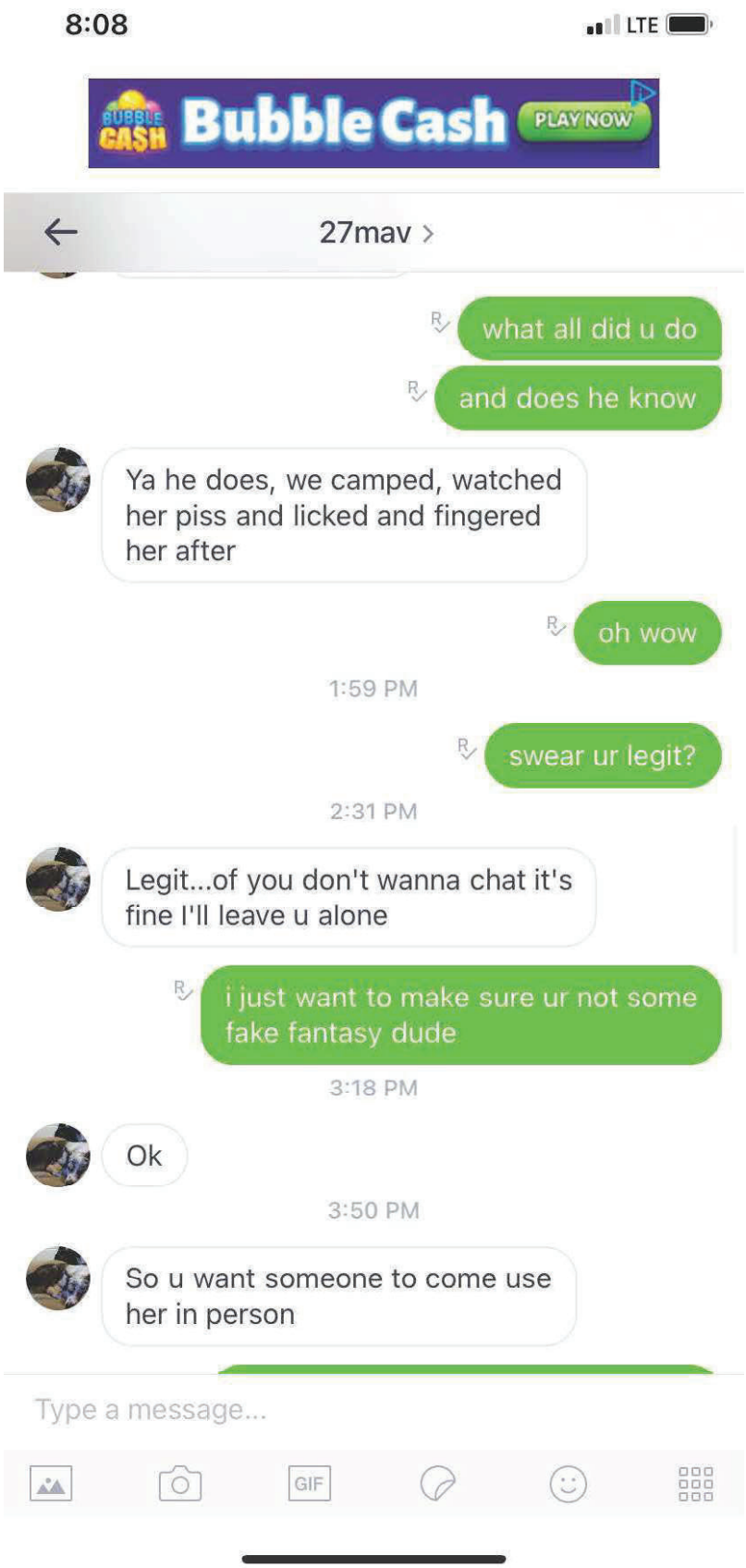

8:08
LTE
MEET 100% REAL PEOPLE
27mav >
Yesterday 8:33 PM
27mav
27mav
255 Days on Kik
Yesterday 8:33 PM
Sharing daug?
hey asl
39 m va
36m fl
what part i lived in fredericksburg before
Charlottesville
oh ok never been
Type a message...
GIF


8:08
LTE
WHAT??!
3 Steps to get free!
27mav >
oh ok never been
Well come take a road trip and bring that daug! Lol
yea right it's winter u come to florida
Ur right lol OMW!
U play w daughter?
been a while
How long?
Why u stop?
what u mean why
Why haven't you played in a while
bc she's 11 now
U don't wanna lick that yng pussy
i definitely want to for sure
Type a message...
GIF

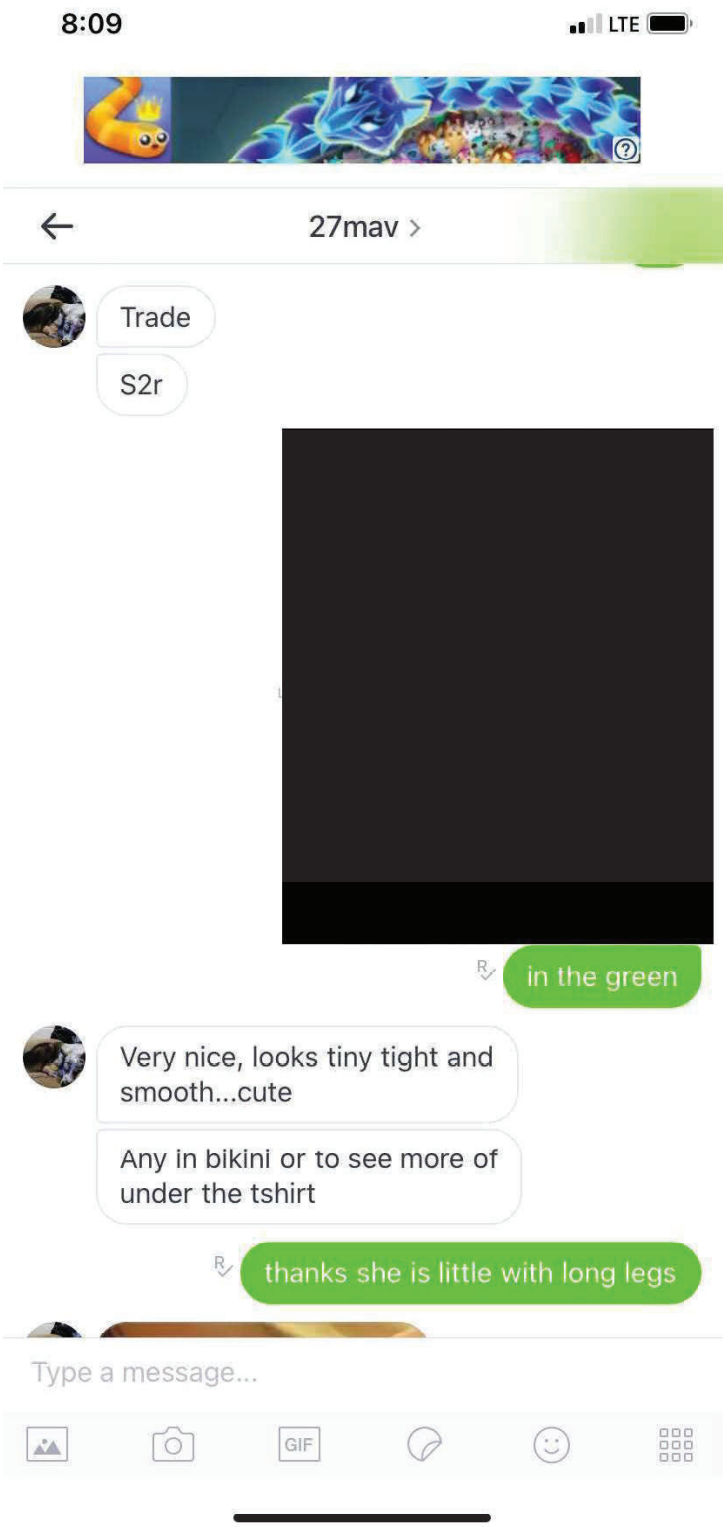

8:08
LTE
WHAT??!
3 Steps to get free!
27mav >
i definitely want to for sure
Use her dirty panties?
panty ain't my thing
Ok
When did u last and what did u do
6:39 AM
Sharing her?
7:51 AM
she would have to agree to it
Pic?
yea i got a ton of her
May I see
do u share
Ya
Type a message...
GIF

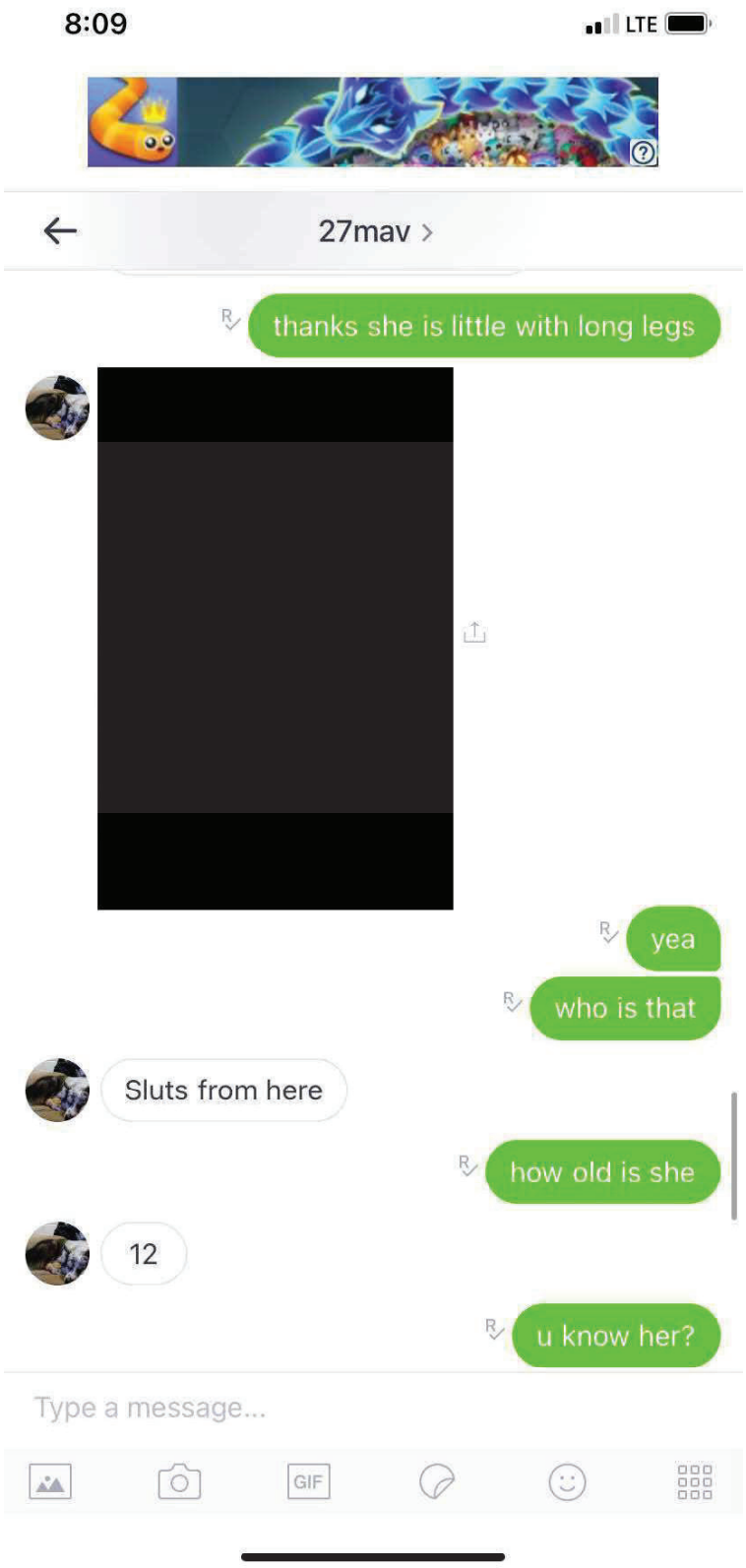

8:08
LTE
WHAT??!
3 Steps to get free!
27mav
Ya
wait what
What?
so ur saying i send u her pics and u share them with others
Ohh hell no of course not unless you tell me to
Sry misunderstood
ok
what kind of pics do u have to share
Yng
how old
Preteen
ok
clothes or no clothes
Type a message...
GIF

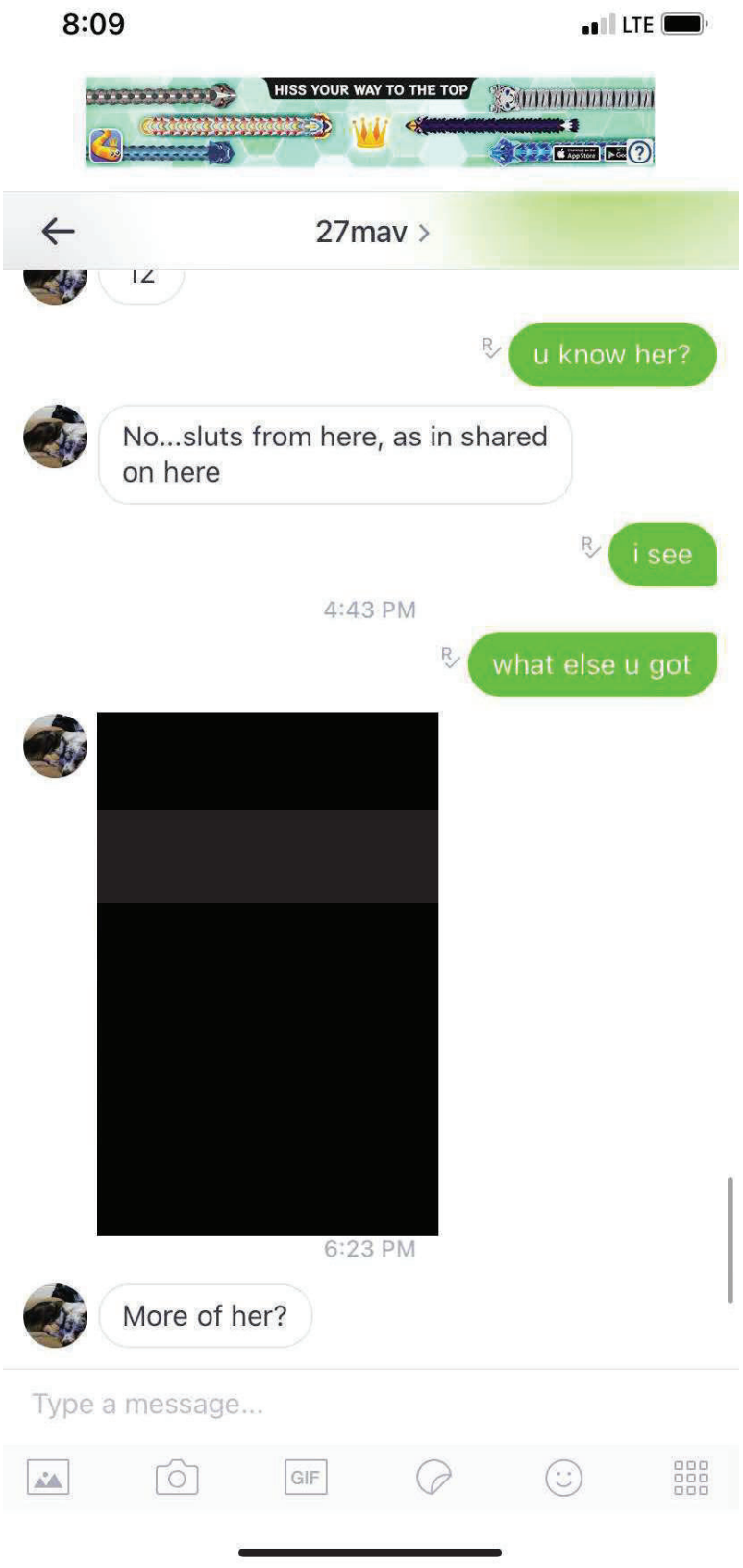

8:08
LTE
Bubble Cash
PLAY NOW
27mav
clothes or no clothes
Both
And vids
ok and with her what are u thinking
Thinking I'd like to see her
irl or online
Maybe both if u want
do u want
If she's hott
do u have any exp with young
Ya
who
Buddy's daughter 14
Type a message...
GIF

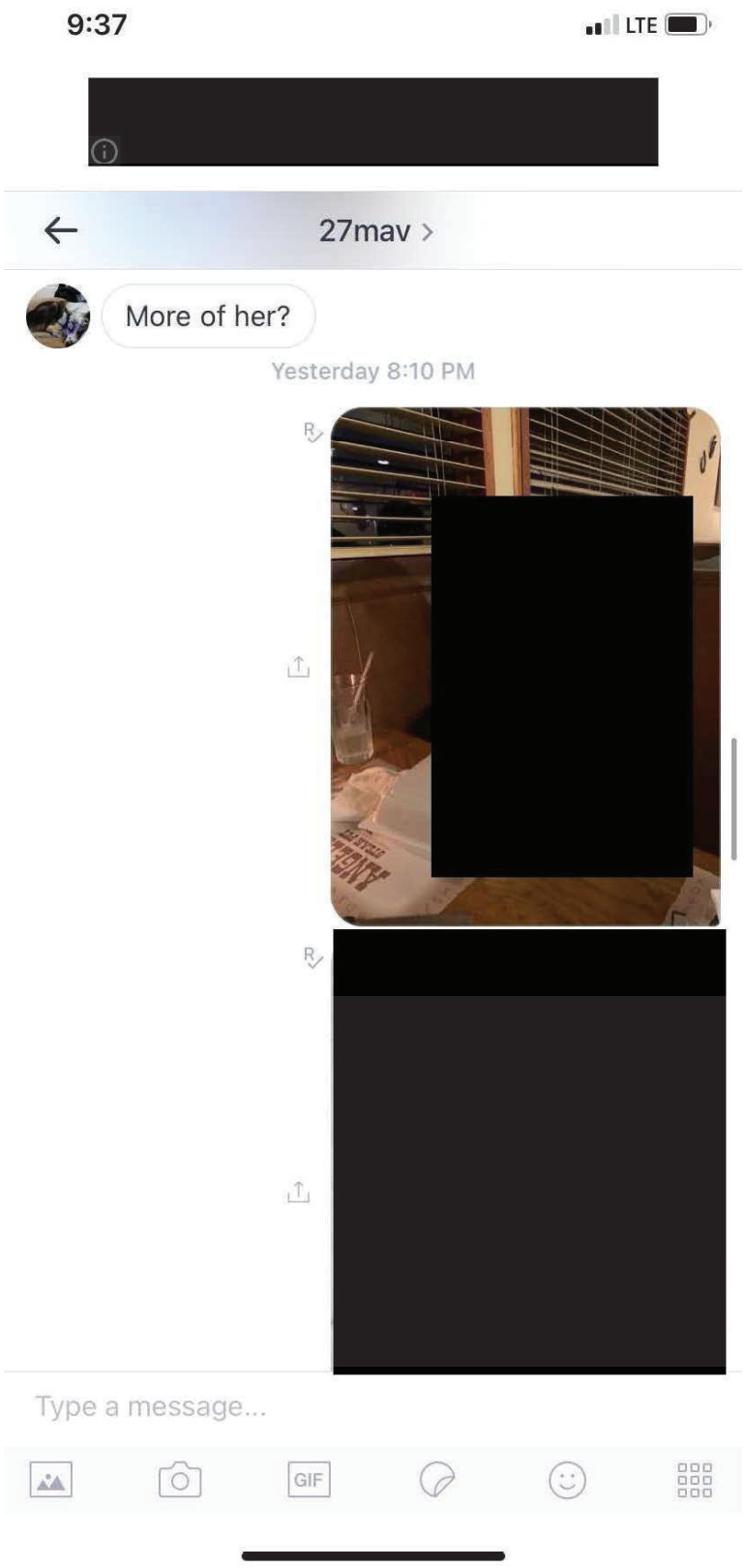

8:08
LTE
Bubble Cash
PLAY NOW
27mav
what all did u do
and does he know
Ya he does, we camped, watched her piss and licked and fingered her after
oh wow
1:59 PM
swear ur legit?
2:31 PM
Legit...of you don't wanna chat it's fine I'll leave u alone
i just want to make sure ur not some fake fantasy dude
3:18 PM
Ok
3:50 PM
So u want someone to come use her in person
Type a message...
GIF


8:08
LTE
27mav >
her in person
the right person maybe but that will take some talking about first
Sure, just wondering
So u have a pic of her?
yea many
May I see
i need proof or assurance ur not gonna screw me first
What do u want
what can u offer
I have yng pics/vids to share
ok
Trade
S2r
Type a message...
GIF

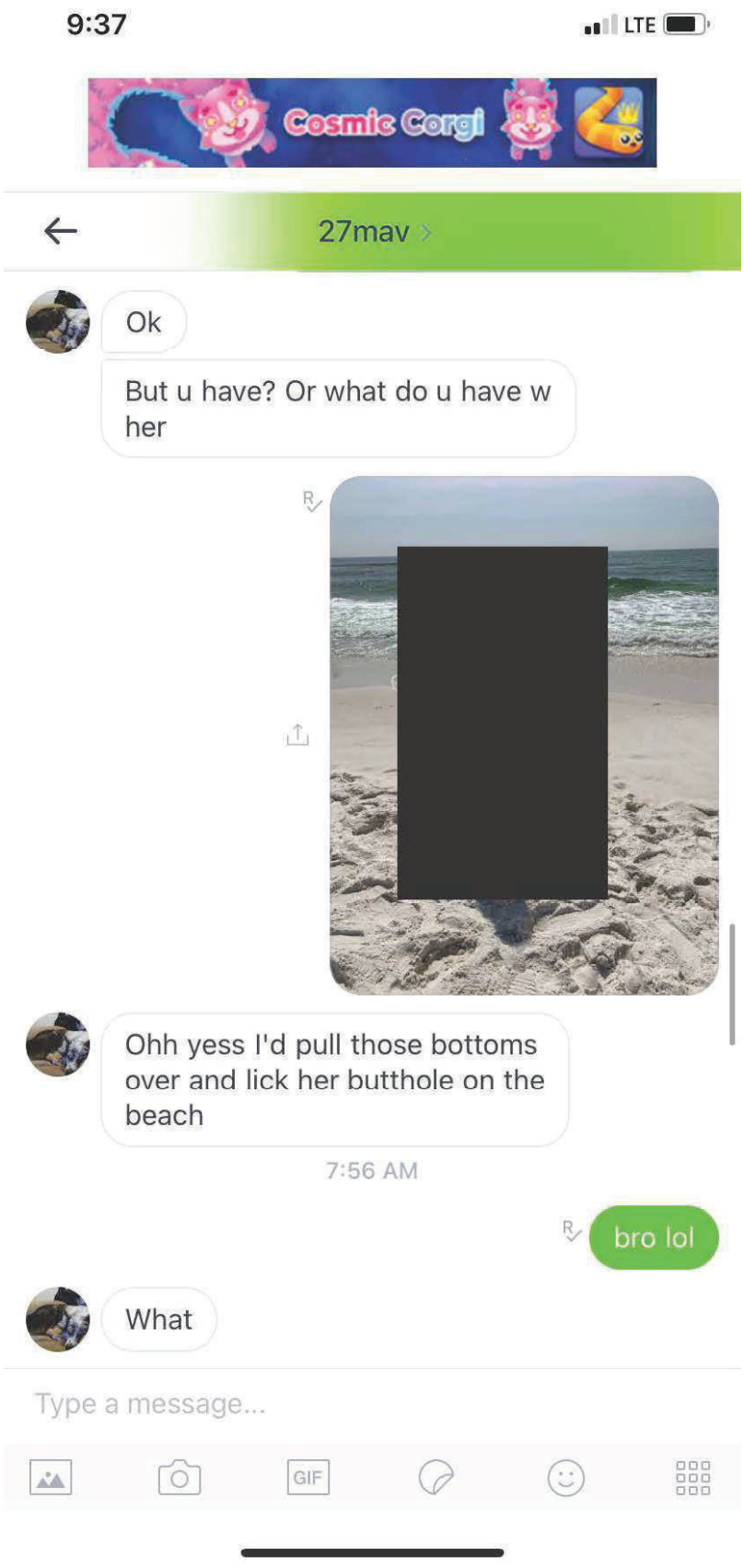

8:09
LTE
27mav
Trade
S2r
in the green
Very nice, looks tiny tight and smooth...cute
Any in bikini or to see more of under the tshirt
thanks she is little with long legs
Type a message...
GIF

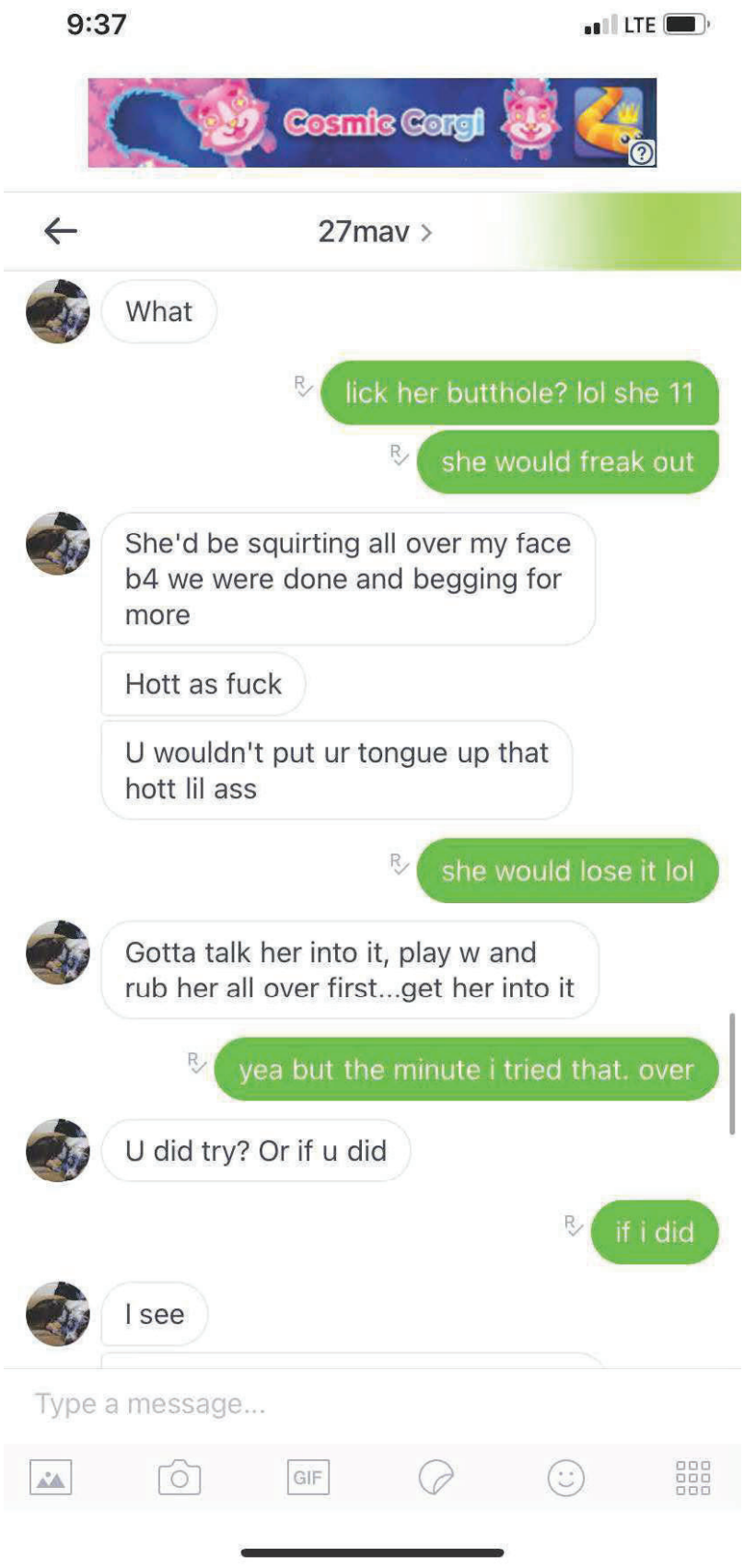

8:09
LTE
27mav
thanks she is little with long legs
yea
who is that
Sluts from here
how old is she
12
u know her?
Type a message...
GIF


8:09
LTE
HISS YOUR WAY TO THE TOP
27mav
u know her?
No...sluts from here, as in shared on here
i see
4:43 PM
what else u got
6:23 PM
More of her?
Type a message...
GIF

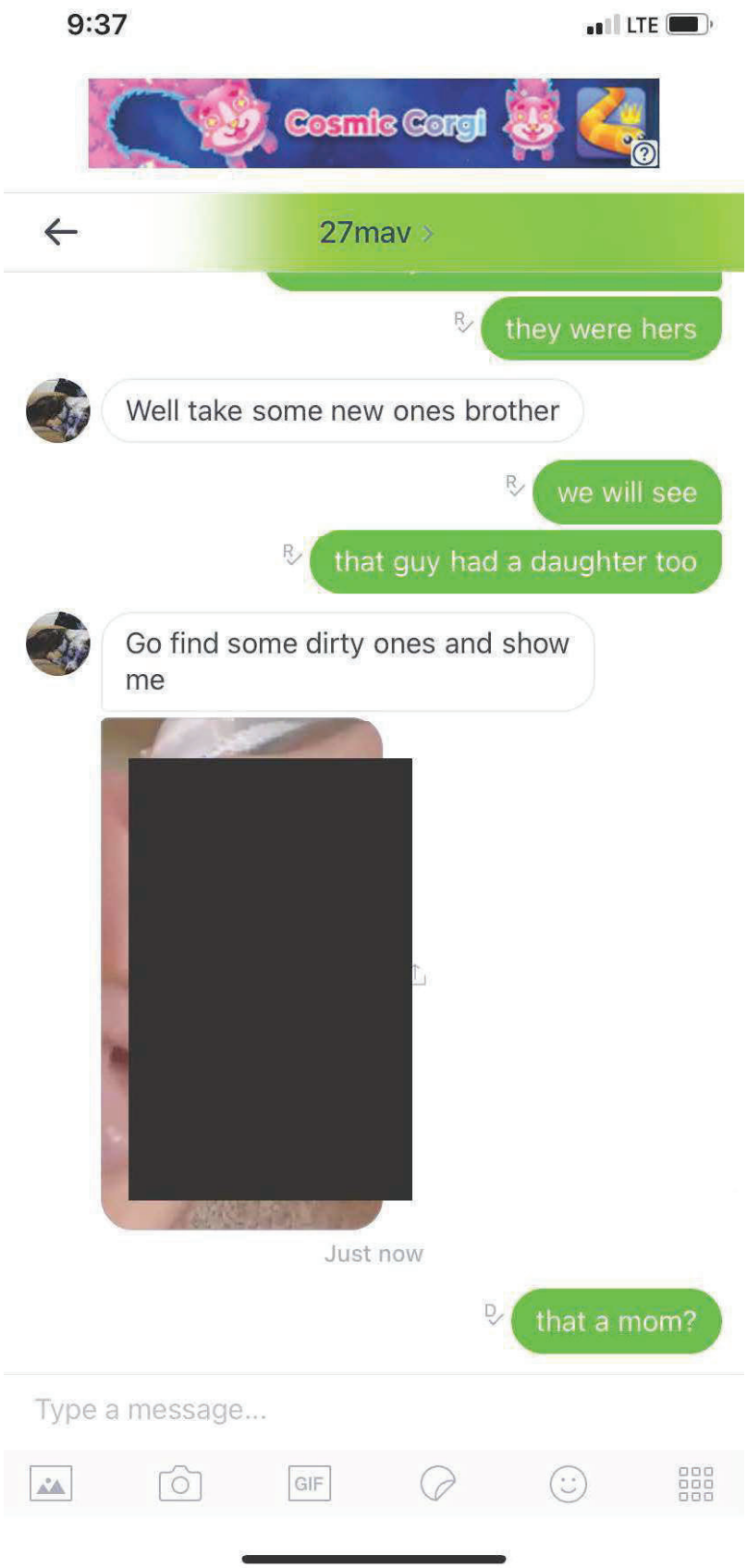

9:37
LTE
[redacted]
27mav >
More of her?
Yesterday 8:10 PM
[redacted]
[redacted]
Type a message...
GIF

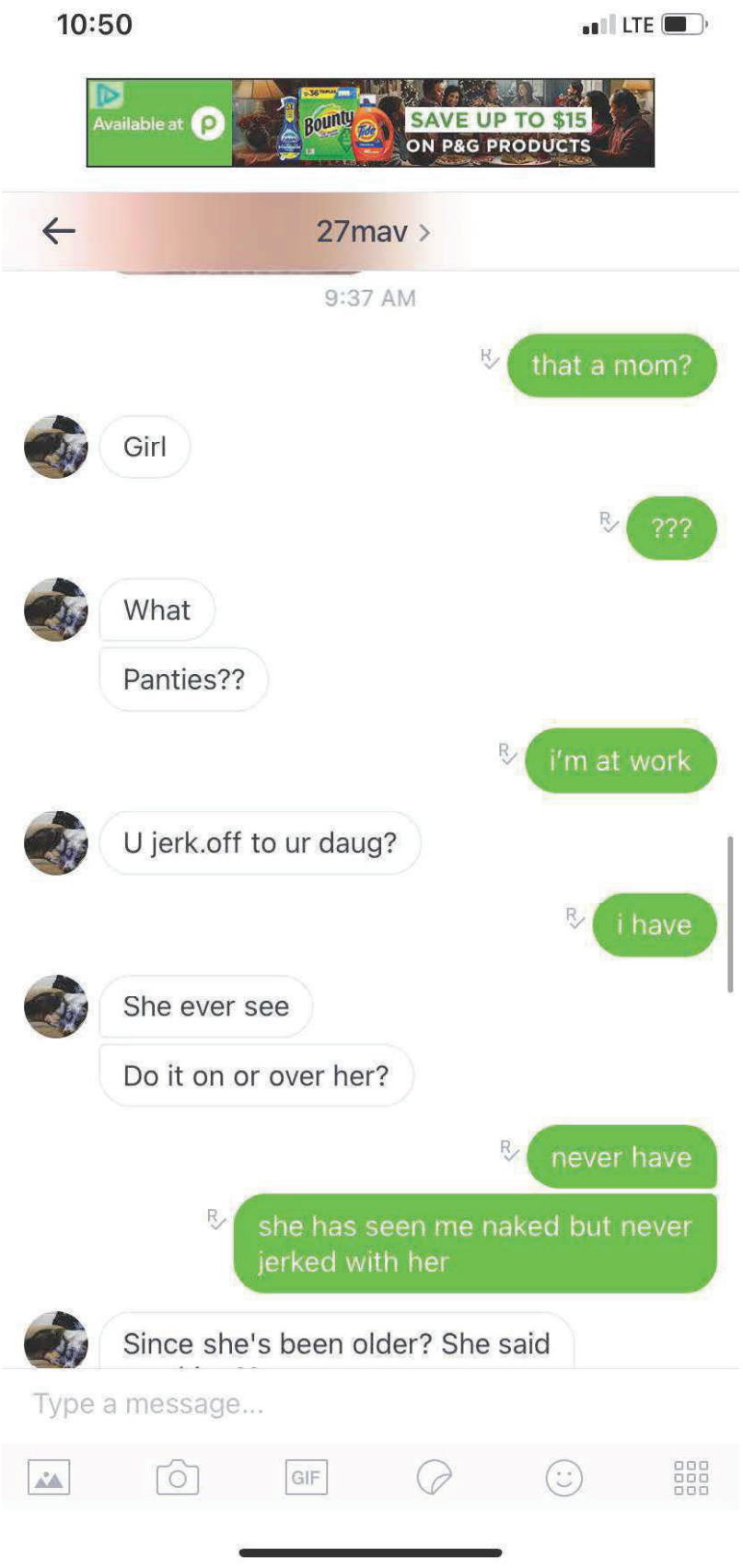

9:37
LTE
Cosmic Corgi
27mav
Mmm I'd sit next to her in the booth at the restaurant and run my hand up her long skinny legs under the table
yea
Mmm yea and up the leg of her shorts as I moved her hand over my cock
what's youngest u got
Idk
U have any naughty of her
how naughty
Nude
i'll send u a bikini of her but no nude rn
Ok
Type a message...
GIF

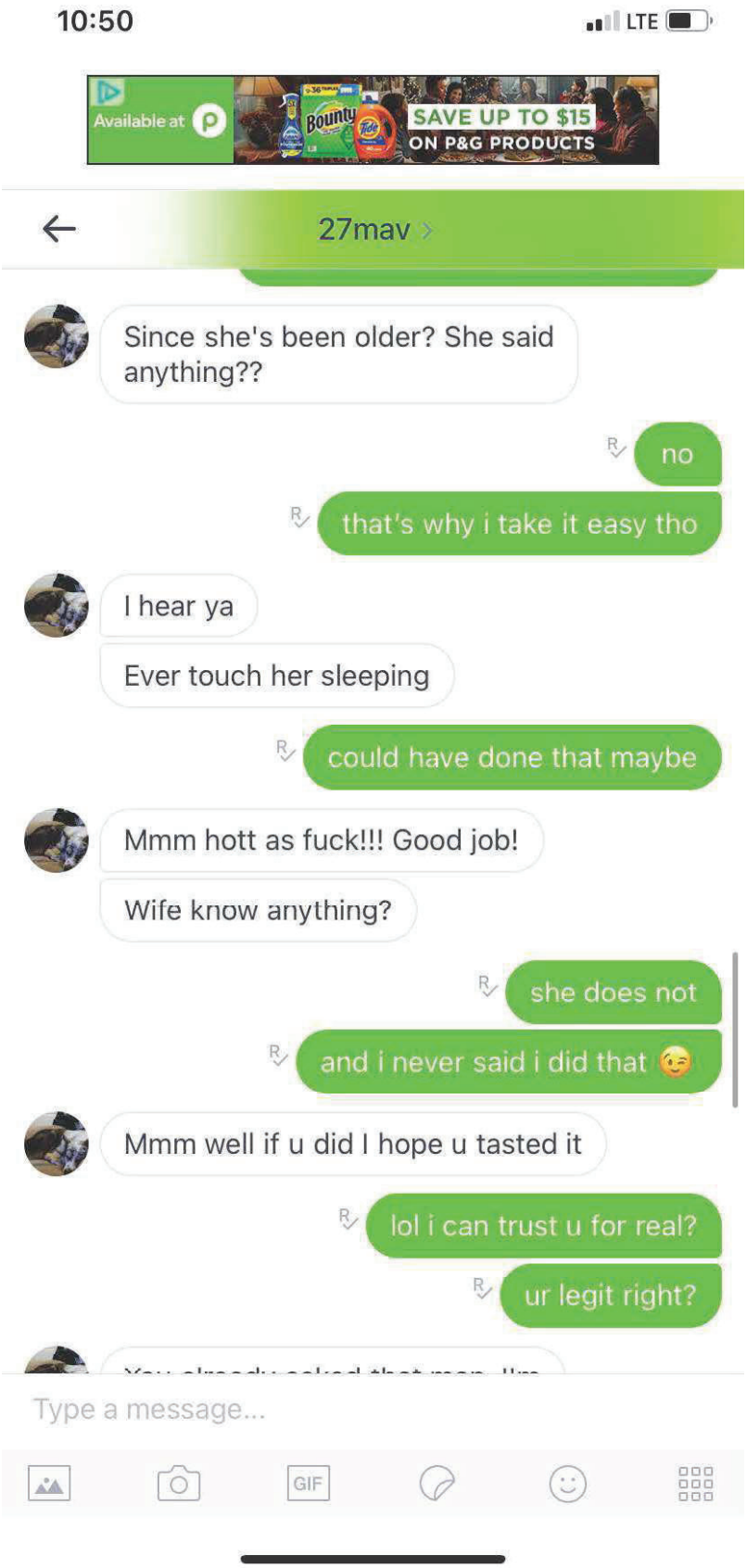

9:37
LTE
Cosmic Corgi
27mav
Ok
But u have? Or what do u have w her
Ohh yess I'd pull those bottoms over and lick her butthole on the beach
7:56 AM
bro lol
What
Type a message...
GIF

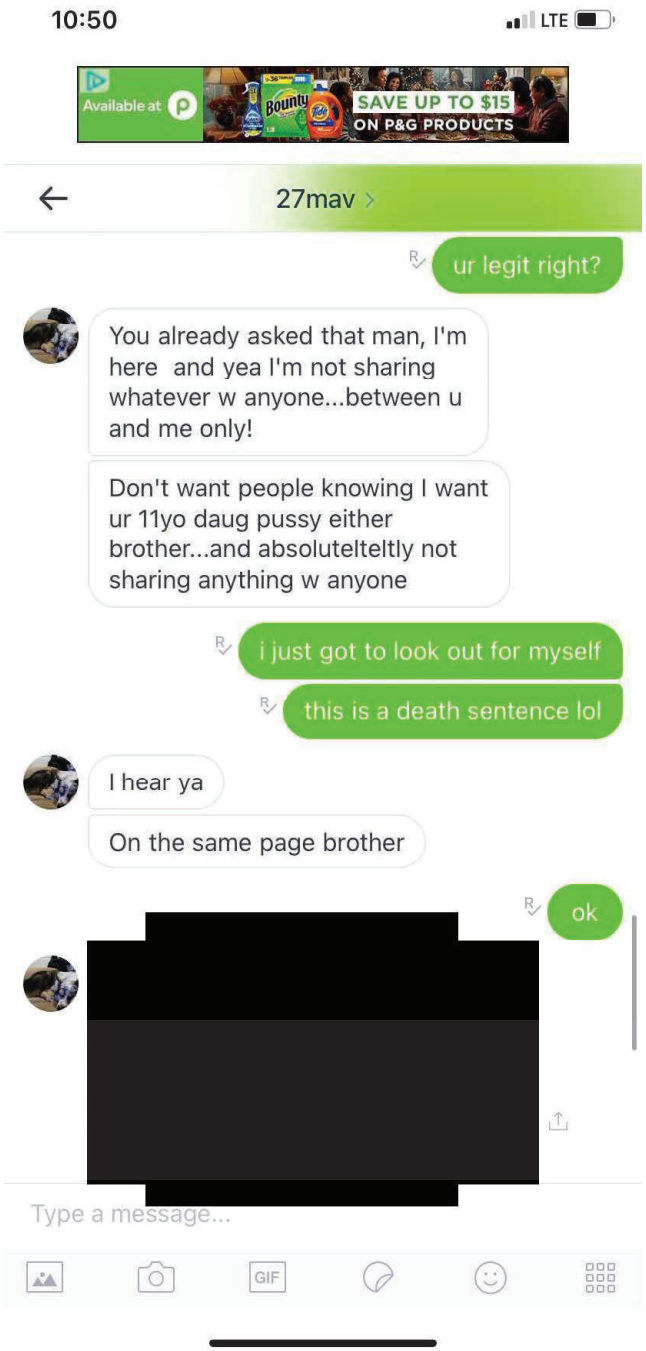

9:37
LTE
Cosmic Corgi
27mav >
What
lick her butthole? lol she 11
she would freak out
She'd be squirting all over my face b4 we were done and begging for more
Hott as fuck
U wouldn't put ur tongue up that hott lil ass
she would lose it lol
Gotta talk her into it, play w and rub her all over first...get her into it
yea but the minute i tried that. over
U did try? Or if u did
if i did
I see
Type a message...
GIF

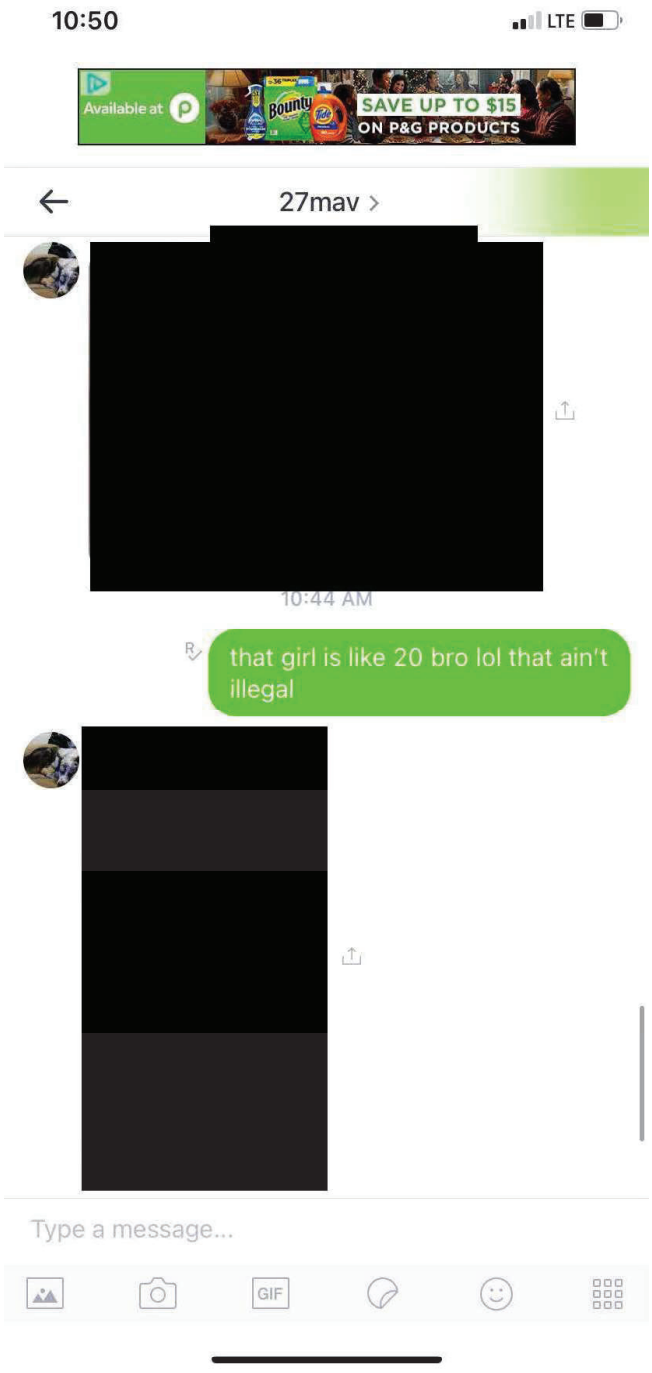

9:37
LTE
Cosmic Corgi
27mav >
I see
U use her dirty wett panties though yea?
use how
Sniff and lick and jerk with
Or wifes?
9:02 AM
Mmm yess are they dirty brother
lol i took that like a year ago for somebody on here
they were hers
Well take some new ones brother
Type a message...
GIF

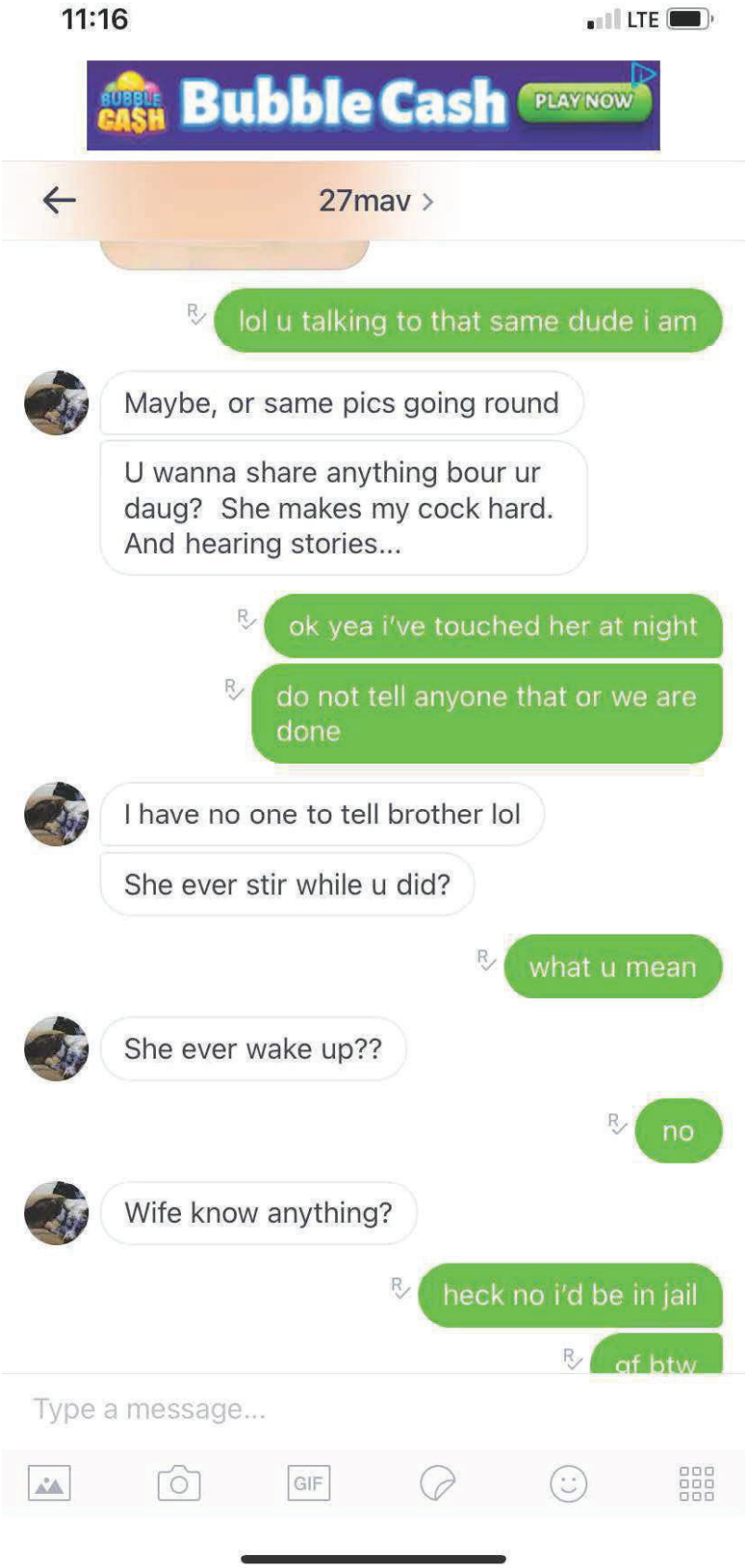

9:37
LTE
Cosmic Corgi
27mav
they were hers
Well take some new ones brother
we will see
that guy had a daughter too
Go find some dirty ones and show me
Just now
that a mom?
Type a message...
GIF


10:50
LTE
Available at
SAVE UP TO $15
ON P&G PRODUCTS
27mav >
9:37 AM
that a mom?
Girl
???
What
Panties??
i'm at work
U jerk.off to ur daug?
i have
She ever see
Do it on or over her?
never have
she has seen me naked but never jerked with her
Since she's been older? She said
Type a message...
GIF


10:50
LTE
Available at
SAVE UP TO $15
ON P&G PRODUCTS
27mav
Since she's been older? She said anything??
no
that's why i take it easy tho
I hear ya
Ever touch her sleeping
could have done that maybe
Mmm hott as fuck!!! Good job!
Wife know anything?
she does not
and i never said i did that
Mmm well if u did I hope u tasted it
lol i can trust u for real?
ur legit right?
Type a message...
GIF


10:50
LTE
Available at
Bounty
SAVE UP TO $15
ON P&G PRODUCTS
27mav
ur legit right?
You already asked that man, I'm here and yea I'm not sharing whatever w anyone...between u and me only!
Don't want people knowing I want ur 11yo daug pussy either brother...and absolutelteltly not sharing anything w anyone
i just got to look out for myself
this is a death sentence lol
I hear ya
On the same page brother
ok
[redacted]
Type a message...
GIF


10:50
LTE
Available at
Bounty
SAVE UP TO $15
ON P&G PRODUCTS
27mav
10:44 AM
that girl is like 20 bro lol that ain't illegal
Type a message...
GIF


11:16
LTE
Bubble Cash
PLAY NOW
27mav
lol u talking to that same dude i am
Maybe, or same pics going round
U wanna share anything bour ur daug? She makes my cock hard. And hearing stories...
ok yea i've touched her at night
do not tell anyone that or we are done
I have no one to tell brother lol
She ever stir while u did?
what u mean
She ever wake up??
no
Wife know anything?
heck no i'd be in jail
gf btw
Type a message...
GIF


11:16
LTE
Bubble Cash
PLAY NOW
27mav >
no
Wife know anything?
heck no i'd be in jail
gf btw
Ohh...gf's kid or urs?
she is my girlfriends
Mm fuck brother, even fucking hotter
why
Playing w other yng pussy w/o gf knowing
Tell me more bout her
like what
Idk anything
lol ok
Type a message...
GIF

23. "27mav" sent at least two photographs and at least two videos of child pornography to the OCE over the internet during the above listed Kik chat. These photographs are redacted for the purposes of this document but in my training and experience are photographs where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct, is indistinguishable from a minor engaging in sexually explicit conduct or has been created or modified to appear than an identifiable minor is engaging in sexually explicit conduct.

24. For example, "27mav" sent the FBI OCE a photograph of an unknown minor female wearing Hello Kitty underwear. The female's genitalia was exposed. As shown above, "27mav" stated that this female was 12 years old. "27mav" also sent the FBI OCE a color video with sound, approximately 55 seconds in length, of a minor[1] female child sitting on a bathroom floor. The child inserts her fingers into her vagina and masturbates throughout the entirety of the video. The child's genitalia and anus are exposed in the video. "27mav" also sent the FBI OCE a color video with sound, approximately 30 seconds in length, of a minor[2] female child. The child inserts her fingers into her vagina and masturbates through the entirety of the video. The child's genitalia and anus are exposed in the video.

25. As also shown in the above chats, "27mav" told the FBI OCE, that he had watched a 14-year-old "piss and licked and fingered her after."

26. A subpoena return from MEDIALAB provided the following information on Kik user "27mav": First Name: 27mav and Email Address: cowboymaverick01@aol.com.

27. A subpoena return from YAHOO, which accepts service for AOL accounts, provided the following information for the email address cowboymaverick01@aol.com: Other

[1] Based on the female's facial features, this female appears to be a minor.
[2] Based on the female's facial features, this female appears to be a minor.

Identities: cowboymaverick01 and cowboymaverick01@aol.com, Full Name: Michael ROOMSBURG, Recovery Email Address: michael.roomsburg@gmail.com, and Recovery Telephone Number: 1 (231) 730-3038.

28. An ACCURINT lookup of telephone number 1 (231) 730-3038 and email address cowboymaverick01@aol.com resolved to the following individual: Name: Michael ROOMSBURG, Social Security Account Number: ---------74, Date of Birth: ---- --, 1985, and Residential Address: 1321 Villa Way, Unit F, Charlottesville, Virginia 22903, i.e. the SUBECT PREMISES. Herein after, ROOMSBURG will also be referred to as SUBJECT 1.

29. Based on surveillance described in the following paragraphs it is believed that the SUBJECT PREMISES is the residence of SUBJECT 1.

30. Surveillance of the SUBJECT PREMISES on February 4, 2025 revealed that "Michael Roomsburg" "and "F" were written on the box outside of the unit. A hand-drawn sign was posted outside of the unit that said "home of 1 dog 1 awesome dad and 1 amazing daughter."

31. During Surveillance of the SUBJECT PREMISES on February 5, 2025, I saw ROOMSBURG exit the apartment building's front door with an Australian shepherd/cattle dog. I am familiar with ROOMSBURG's appearance based on review of his driver's license photograph and photographs on ROOMSBURG's public Facebook account. A 2011 Jeep Compass bearing Virginia license plate UBD-2229 was present at the apartment complex. The aforementioned vehicle was registered to ROOMSBURG at that address.

32. On February 4, 2025, law enforcement interviewed a member of the apartment management team who stated ROOMSBURG resided at the SUBJECT PREMISES, with an Australian shepherd dog. The profile photograph of Kik user "27mav" was of an Australian breed dog. On February 5, 2025, law enforcement contacted that apartment management team member

and asked about ROOMSBURG's daughter. Law enforcement was advised she stayed with ROOMSBURG "on occasion," but not during the week as she attended school.

COMPUTERS, CELLULAR DEVICES, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

33. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, to include cellular devices. Thus, the warrant applied for would authorize the seizure of electronic storage media and the copying and searching of electronically stored information on that media, all under Rule 41(e)(2)(B).

34. If SUBJECT 1 is present at the time of the search, the warrant would also authorize the search of SUBJECT 1's person for SUBJECT 1's electronic devices, the seizure of any such devices, and the copying and searching of any such devices.

35. *Probable cause.* I submit that if a computer, cellular device, or storage medium is found on the SUBJECT PREMISES or on the person of SUBJECT 1 within the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer, cellular device, or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or

years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

36. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how

computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer, cellular, and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of

session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer, cellular, or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated

camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular

thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to distribute or download CEM, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

37. *Necessity of seizing or copying entire computers, cellular, or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

38. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

AUTHORIZATION FOR FINGERPRINT UNLOCK OF APPLE IPHONE

39. In my training and experience, it is likely that the SUBJECT PREMISES may contain at least one Apple brand device, such as an iPhone or iPad. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

40. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the

device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

41. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

42. The passcode or password that would unlock any devices found at the SUBJECT PREMISES is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) of the devices found during the search of the SUBJECT PREMISES to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

43. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is

also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the SUBJECT PREMISES to press their finger(s) against the Touch ID sensor of the locked Apple device(s) found during the search of the Subject Premises in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID. Based on these facts and my training and experience, it is likely that MICHAEL ROOMSBURG is a user of any devices at the SUBJECT PREMISES and thus that their fingerprints are among those that are able to unlock the device via Touch ID.

44. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock any devices found in the SUBJECT PREMISES as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

45. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the SUBJECT PREMISES to the Touch ID sensor of devices found at SUBJECT PREMISES , such as an iPhone or iPad, found at the SUBJECT PREMISES for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

CONCLUSION

46. Based on the above there is probable cause to believes that SUBJECT 1 received and possessed child pornography in violation of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B). There is further probable cause to believe that contraband as well as evidence, fruits and instrumentalities of these crimes are located within the SUBJECT PREMISES.

OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

s/Jade S. Laughlin
Jade S. Laughlin, Special Agent
Federal Bureau of Investigation

Received by reliable electronic means and sworn and attested to by telephone on this 7th day of February 2025.

HONORABLE JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE